The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

9/18/2013

SUBJECT:

Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Firefox versions prior to 24.0
- Firefox Extended Support Release (ESR) versions prior to 17.0.9
- Thunderbird versions prior to 24.0
- Thunderbird Extended Support Release (ESR) versions prior to 17.0.9
- SeaMonkey versions prior to 2.21

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey. The details of these vulnerabilities are as follows:

- Multiple memory-corruption vulnerabilities exist in the browser engine that could lead to arbitrary code execution. [CVE-2013-1718, CVE-2013-1719] [MFSA 2013-76]
- A heap buffer-overflow vulnerability occurs because the HTML5 Tree Builder does not properly store state when interacting with template elements. Specifically, this issue affects the 'nsHtml5TreeBuilder::resetTheInsertionMode()' function. [CVE-2013-1720] [MFSA 2013-77]
- An integer-overflow vulnerability exists in the Almost Native Graphics Layer Engine (ANGLE) library. Specifically, this issue affects the 'drawLineLoop()' function. [CVE-2013-1721] [MFSA 2013-78]
- A use-after-free vulnerability occurs when cloning of stylesheets. Specifically this issue exists in the Animation Manage. [CVE-2013-1722] [MFSA 2013-79]
- A denial-of-service vulnerability affects the application. Specifically, this issue occurs because the NativeKey widget continues to handle key messages after widget is destroyed. [CVE-2013-1723] [MFSA 2013-80]
- A use-after-free vulnerability occurs when using a 'select' element in a form after it has been destroyed. Specifically, this issue affects the 'mozilla::dom::HTMLFormElement::IsDefaultSubmitElement()' function. [CVE-2013-1724] [MFSA 2013-81]
- A memory-corruption vulnerability occurs when calling a Javascript object with an uninitialized compartment. [CVE-2013-1725][MFSA 2013-82]
- A security-bypass vulnerability exists because the Mozilla Updater does not write-lock the MAR update file when it is in use by the Updater. [CVE-2013-1726] [MFSA 2013-83]
- A same-origin security-bypass vulnerability affects the application. An attacker can exploit this issue to violate same-origin policy for local files using 'file://'through the use of symbolic links. NOTE: This issue only effects Firefox for Android [CVE-2013-1727] [MFSA 2013-84]
- A security vulnerability exists due to uninitialized data in IonMonkey. Specifically, this issue occurs when running the engine in Valgrind mode. [CVE-2013-1728] [MFSA 2013-85]
- An information-disclosure vulnerability exists in the NVIDIA OS X graphic drivers. An attacker can exploit this issue to disclose WebGL information. [CVE-2013-1729] [MFSA 2013-86]
- A local insecure-file-permissions vulnerability because Firefox for Android loads a shared object (.so) library in order to enable GL tracing from a world writable location. [CVE-2013-1731] [MFSA 2013-87]
- A security vulnerability exists in the 'nsXBLBinding::DoInitJSClass()' function. Specifically, this issue occurs when moving certain XBL-backed nodes from a document into the replacement document created by 'document.open()'. [CVE-2013-1730] [MFSA 2013-88]
- A buffer-overflow vulnerability affects the application. Specifically, this issue occurs in the 'nsFloatManager::GetFlowArea()' function when combining lists, floats, and multiple columns.[CVE-2013-1732] [MFSA 2013-89]
- Multiple memory-corruption vulnerabilities occur that are related with scrolling. Specifically, these issues affect the 'mozilla::layout::ScrollbarActivity()' and 'nsGfxScrollFrameInner::IsLTR()' functions. [CVE-2013-1735, CVE-2013-1736] [MFSA 2013-90]
- A security vulnerability exists because user-defined properties on DOM proxies get the wrong 'this' object. [CVE-2013-1737] [MFSA 2013-91]
- A security vulnerability exists because of a GC hazard with default compartments and frame chain restoration. [CVE-2013-1738] [MFSA 2013-92]

Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade vulnerable Mozilla products immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Mozilla:

http://www.mozilla.org/security/announce/2013/mfsa2013-76.html

http://www.mozilla.org/security/announce/2013/mfsa2013-77.html

http://www.mozilla.org/security/announce/2013/mfsa2013-78.html

http://www.mozilla.org/security/announce/2013/mfsa2013-79.html

http://www.mozilla.org/security/announce/2013/mfsa2013-80.html

http://www.mozilla.org/security/announce/2013/mfsa2013-81.html

http://www.mozilla.org/security/announce/2013/mfsa2013-82.html

http://www.mozilla.org/security/announce/2013/mfsa2013-83.html

http://www.mozilla.org/security/announce/2013/mfsa2013-84.html

http://www.mozilla.org/security/announce/2013/mfsa2013-85.html

http://www.mozilla.org/security/announce/2013/mfsa2013-86.html

http://www.mozilla.org/security/announce/2013/mfsa2013-87.html

http://www.mozilla.org/security/announce/2013/mfsa2013-88.html

http://www.mozilla.org/security/announce/2013/mfsa2013-89.html

http://www.mozilla.org/security/announce/2013/mfsa2013-90.html

http://www.mozilla.org/security/announce/2013/mfsa2013-91.html

http://www.mozilla.org/security/announce/2013/mfsa2013-92.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1718

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1719

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1720

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1721

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1722

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1723

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1724

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1725

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1726

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1727

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1728

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1729

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1730

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1731

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1732

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1735

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1736

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1737

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1738

SecurityFocus:

http://www.securityfocus.com/bid/62447